UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/028,017	12/21/2001	Jon W. Hamilton	021971.0164	2955

7590 09/16/2005

Matthew B. Talpis, Esq.
Baker Botts L.L.P.
Suite 600
2001 Ross Avenue
Dallas, TX 75201-2980

EXAMINER	
PARTHASARATHY, PRAMILA	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 09/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/028,017	HAMILTON, JON W.	
	Examiner	Art Unit	
	Pramila Parthasarathy	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 June 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *5/22/2002*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on June 24, 2003. Claims 1 – 30 are pending.

Information Disclosure Statement

2. An initialed copy of the information disclosure statement (IDS) submitted on 5/22/2002 is attached to this office action.

Claim Objections

3. Claims 1, 9, 23 and 30 are objected to because of the following informalities:

Claim 1 recites "...generating an encrypted image based the P box ...". Please replace with "...generating an encrypted image based on the P box ...".

Claim 9, 23 and 30 recites "...reconstruct at least one ...". Please replace with "...reconstructing at least one ...".

Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 9, 23 and 30 recite the limitation "the first reverse S box, the second reverse S box" in lines 11-12 of the claims. There is insufficient antecedent basis for this limitation in the claim. Examiner reads as "the reverse S1 box, the reverse S2 box"

The dependent claims 10 – 14 and 24 – 28 are rejected at least by virtue of their dependency on the independent claims 9 and 23, and by other reason set forth in this office action.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1 – 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leech (U.S. Patent Number 5,745,577, hereafter "Leech") in view of Murphy et al. (U.S. Patent Number 5,799,082, hereafter "Murphy").

6. Regarding Claim 1, Leech teaches providing an unencrypted image; partitioning the unencrypted image into at least one partition (Leech Summary and Column 4 lines 14 – 18);

applying a P box to each partition (Leech Summary and Column 6 lines 45 – 66);

applying a first S box to each partition (Leech Summary and Column 4 lines 14 – 57);

applying a second S box to each partition (Leech Summary and Column 4 lines 14 – 57);

generating an encrypted image based the P box, the first S box and the second S box (Leech Summary; Column 4 lines 14 – 57 and Column 6 lines 45 – 66).

Leech discloses an encryption method of cryptographically transforming between plaintext and ciphertext in data block through a set of a plurality of consecutive transformation rounds. Leech does not explicitly disclose that the data is an image. However, Murphy discloses apparatus for capturing and authenticating an image using a digital camera wherein position information maybe encrypted using an encryption key and encryption/decryption process may be a single key process such as DES (Murphy Summary and Column 12 line 63 – Column 13 line 37). Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the teaching of Murphy to partition the unencrypted image and encrypting the portioned image using the encrypting algorithm taught by Leech because one having ordinary skill in the art would want to provide a cryptosystem which employs two sets of s-boxes and p-box for higher degree of resistance to cryptanalysis.

Motivation to combine the invention of Leech with Murphy teachings comes from the need for securing data by cryptographically transforming data (image) using two different s-boxes to provide resistance to cryptanalysis. Leech provides a discussion of the need for data encryption methods but are silent as to the specific details of the technical manipulation involved for image, see Leech Background information and Column 3 line 2 – Column 5 line 46. It would have been obvious to one of ordinary skill in the art to combine Leech with Murphy because security through encryption and authentication is needed for images of Leech and Murphy provides some details of how to provide security for images with the encryption methods. O'Shea could have been modified by Leech because Leech provides a secure and specialized encryption methods of text data and O'Shea discloses a system for manipulating image data.

7. Regarding Claim 9, Leech teaches providing an encrypted digital image; reconstruct least one partition based on the encrypted digital image (Leech Summary and Column 4 lines 14 – 18);

reconstruct at least one trajectory associated with the encrypted digital image (Leech Summary and Column 4 lines 14 – 18);

applying a reverse S 2 box to the partitions based on the trajectories (Leech Summary and Column 4 lines 14 – 57);

applying a reverse S1 box to the partitions (Leech Summary and Column 4 lines 14 – 57);

applying a reverse P box to the partitions(Leech Summary and Column 6 lines 45 – 66); and generating an unencrypted digital image based on the first reverse S box, the second reverse S box and the reverse P box (Leech Summary; Column 4 lines 14 – 57 and Column 6 lines 45 – 66).

Leech discloses an encryption method of cryptographically transforming between plaintext and ciphertext in data block through a set of a plurality of consecutive transformation rounds. Leech does not explicitly disclose that the data is an image. However, Murphy discloses apparatus for capturing and authenticating an image using a digital camera wherein position information maybe encrypted using an encryption key and encryption/decryption process may be a single key process such as DES (Murphy Summary and Column 12 line 63 – Column 13 line 37). Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the teaching of Murphy to partition the unencrypted image and encrypting the portioned image using the encrypting algorithm taught by Leech because one having ordinary skill in the art would want to provide a cryptosystem which employs two sets of s-boxes and p-box for higher degree of resistance to cryptanalysis.

Motivation to combine the invention of Leech with Murphy teachings comes from the need for securing data by cryptographically transforming data (image) using two different s-boxes to provide resistance to cryptanalysis. Leech provides a discussion of the need for data encryption methods but are silent as to the specific details of the technical manipulation involved for image, see Leech Background information and

Column 3 line 2 – Column 5 line 46. It would have been obvious to one of ordinary skill in the art to combine Leech with Murphy because security through encryption and authentication is needed for images of Leech and Murphy provides some details of how to provide security for images with the encryption methods. O'Shea could have been modified by Leech because Leech provides a secure and specialized encryption methods of text data and O'Shea discloses a system for manipulating image data.

8. Regarding Claim 15, Leech teaches provide an unencrypted image; partition the unencrypted image at least one partition (Leech Summary and Column 4 lines 14 – 18);

apply a P box to each partition (Leech Summary and Column 6 lines 45 – 66);

apply a first S box to each partition (Leech Summary and Column 4 lines 14 – 57);

apply a second S box to each partition (Leech Summary and Column 4 lines 14 – 57); and generate an encrypted image based the P box, the first S box and the second S box (Leech Summary; Column 4 lines 14 – 57 and Column 6 lines 45 – 66).

Leech discloses an encryption method of cryptographically transforming between plaintext and ciphertext in data block through a set of a plurality of consecutive transformation rounds. Leech does not explicitly disclose that the data is an image. However, Murphy discloses apparatus for capturing and authenticating an image using a digital camera wherein position information maybe encrypted using an encryption key and encryption/decryption process may be a single key process such as DES (Murphy Summary and Column 12 line 63 – Column 13 line 37). Therefore, it would have been

obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the teaching of Murphy to partition the unencrypted image and encrypting the portioned image using the encrypting algorithm taught by Leech because one having ordinary skill in the art would want to provide a cryptosystem which employs two sets of s-boxes and p-box for higher degree of resistance to cryptanalysis.

Motivation to combine the invention of Leech with Murphy teachings comes from the need for securing data by cryptographically transforming data (image) using two different s-boxes to provide resistance to cryptanalysis. Leech provides a discussion of the need for data encryption methods but are silent as to the specific details of the technical manipulation involved for image, see Leech Background information and Column 3 line 2 – Column 5 line 46. It would have been obvious to one of ordinary skill in the art to combine Leech with Murphy because security through encryption and authentication is needed for images of Leech and Murphy provides some details of how to provide security for images with the encryption methods. O'Shea could have been modified by Leech because Leech provides a secure and specialized encryption methods of text data and O'Shea discloses a system for manipulating image data.

9. Regarding Claim 23, Leech teaches providing an encrypted digital image; reconstruct at least one partition based the encrypted digital image (Leech Summary and Column 4 lines 14 – 18);

reconstruct least one trajectory associated with the encrypted digital image (Leech Summary and Column 4 lines 14 – 18);

applying a reverse S 2 box to the partitions based on the trajectories (Leech Summary and Column 4 lines 14 – 18);

applying a reverse S1 box to the partitions (Leech Summary and Column 4 lines 14 – 18);

applying a reverse P box to the partitions (Leech Summary and Column 4 lines 14 – 18); and

generating an unencrypted digital image based on the first reverse S box, the second reverse S box and reverse P box (Leech Summary; Column 4 lines 14 – 57 and Column 6 lines 45 – 66).

Leech discloses an encryption method of cryptographically transforming between plaintext and ciphertext in data block through a set of a plurality of consecutive transformation rounds. Leech does not explicitly disclose that the data is an image. However, Murphy discloses apparatus for capturing and authenticating an image using a digital camera wherein position information maybe encrypted using an encryption key and encryption/decryption process may be a single key process such as DES (Murphy Summary and Column 12 line 63 – Column 13 line 37). Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the teaching of Murphy to partition the unencrypted image and encrypting the portioned image using the encrypting algorithm taught by Leech because one

having ordinary skill in the art would want to provide a cryptosystem which employs two sets of s-boxes and p-box for higher degree of resistance to cryptanalysis.

Motivation to combine the invention of Leech with Murphy teachings comes from the need for securing data by cryptographically transforming data (image) using two different s-boxes to provide resistance to cryptanalysis. Leech provides a discussion of the need for data encryption methods but are silent as to the specific details of the technical manipulation involved for image, see Leech Background information and Column 3 line 2 – Column 5 line 46. It would have been obvious to one of ordinary skill in the art to combine Leech with Murphy because security through encryption and authentication is needed for images of Leech and Murphy provides some details of how to provide security for images with the encryption methods. O'Shea could have been modified by Leech because Leech provides a secure and specialized encryption methods of text data and O'Shea discloses a system for manipulating image data.

10. Regarding Claim 29, Leech teaches means for providing an unencrypted image; means for partitioning the unencrypted image into at least one partition (Leech Summary and Column 4 lines 14 – 18);

means for applying P box to each partition (Leech Summary and Column 4 lines 14 – 57);

means for applying a first S box to each partition (Leech Summary and Column 4 lines 14 – 57);

means for applying second S box to each partition (Leech Summary and Column 4 lines 14 – 57); and

means for generating an encrypted image based the P box, the first S box and the second S box (Leech Summary; Column 4 lines 14 – 57 and Column 6 lines 45 – 66);

Leech discloses an encryption method of cryptographically transforming between plaintext and ciphertext in data block through a set of a plurality of consecutive transformation rounds. Leech does not explicitly disclose that the data is an image. However, Murphy discloses apparatus for capturing and authenticating an image using a digital camera wherein position information maybe encrypted using an encryption key and encryption/decryption process may be a single key process such as DES (Murphy Summary and Column 12 line 63 – Column 13 line 37). Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the teaching of Murphy to partition the unencrypted image and encrypting the portioned image using the encrypting algorithm taught by Leech because one having ordinary skill in the art would want to provide a cryptosystem which employs two sets of s-boxes and p-box for higher degree of resistance to cryptanalysis.

Motivation to combine the invention of Leech with Murphy teachings comes from the need for securing data by cryptographically transforming data (image) using two different s-boxes to provide resistance to cryptanalysis. Leech provides a discussion of the need for data encryption methods but are silent as to the specific details of the

technical manipulation involved for image, see Leech Background information and Column 3 line 2 – Column 5 line 46. It would have been obvious to one of ordinary skill in the art to combine Leech with Murphy because security through encryption and authentication is needed for images of Leech and Murphy provides some details of how to provide security for images with the encryption methods. O'Shea could have been modified by Leech because Leech provides a secure and specialized encryption methods of text data and O'Shea discloses a system for manipulating image data.

11. Regarding Claim 30, Leech teaches means for providing an encrypted digital image; means for reconstruct at least one partition based on the encrypted digital image(Leech Summary and Column 4 lines 14 – 18);

means for reconstruct at least one trajectory associated with the encrypted digital image (Leech Summary and Column 4 lines 14 – 18);

means for applying a reverse S 2 box to the partitions based on the trajectories (Leech Summary and Column 4 lines 14 – 18);

means for applying a reverse S1 box to the partitions (Leech Summary and Column 4 lines 14 – 18);

means for applying a reverse P box to the partitions (Leech Summary and Column 4 lines 14 – 18); and

means for generating an unencrypted digital image based on the first reverse S box, the second reverse S box and the reverse P box (Leech Summary; Column 4 lines 14 – 57 and Column 6 lines 45 – 66).

Leech discloses an encryption method of cryptographically transforming between plaintext and ciphertext in data block through a set of a plurality of consecutive transformation rounds. Leech does not explicitly disclose that the data is an image. However, Murphy discloses apparatus for capturing and authenticating an image using a digital camera wherein position information maybe encrypted using an encryption key and encryption/decryption process may be a single key process such as DES (Murphy Summary and Column 12 line 63 – Column 13 line 37). Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the teaching of Murphy to partition the unencrypted image and encrypting the portioned image using the encrypting algorithm taught by Leech because one having ordinary skill in the art would want to provide a cryptosystem which employs two sets of s-boxes and p-box for higher degree of resistance to cryptanalysis.

Motivation to combine the invention of Leech with Murphy teachings comes from the need for securing data by cryptographically transforming data (image) using two different s-boxes to provide resistance to cryptanalysis. Leech provides a discussion of the need for data encryption methods but are silent as to the specific details of the technical manipulation involved for image, see Leech Background information and Column 3 line 2 – Column 5 line 46. It would have been obvious to one of ordinary skill in the art to combine Leech with Murphy because security through encryption and authentication is needed for images of Leech and Murphy provides some details of how to provide security for images with the encryption methods. O'Shea could have been

modified by Leech because Leech provides a secure and specialized encryption methods of text data and O'Shea discloses a system for manipulating image data.

12. Claims 2 and 16 are rejected applied as above in rejecting Claims 1 and 15. Furthermore, Leech in view of Murphy teaches generating the unencrypted image at a camera (Murphy Summary and Column 9 line 34 – Column 10 line 57).

13. Claims 3 and 17 are rejected applied as above in rejecting Claims 1 and 15. Furthermore, Leech in view of Murphy teaches determining a dimension of the unencrypted image; partitioning the image portion into at least one image partition blocks based on a minimum partition block size and a maximum partition block size; partitioning the text portion into at least one text partition blocks based on the minimum partition block size and the maximum partition block size; indexing the image partition blocks; and indexing the text partition blocks (Leech Summary; Column 4 lines 14 – 57 and Column 6 lines 45 – 66 and Murphy Summary and Column 9 line 34 – Column 10 line 57).

14. Claims 5, 13, 19, and 27 are rejected applied as above in rejecting Claims 1, 9, 15 and 23. Furthermore, Leech in view of Murphy teaches applying a bit enumeration to each partition; permuting a plurality of bits in each partition; and rotating a plurality of nibbles in each partition (Leech Summary; Column 4 lines 14 – 57 and Column 6 lines 45 – 66 and Murphy Summary and Column 9 line 34 – Column 10 line 57).

15. Claims 6, 11, 20 and 25 are rejected applied as above in rejecting Claims 1, 9, 15 and 23. Furthermore, Leech in view of Murphy teaches applying a first non-linear feedback shift register to the partition; selecting a nibble from the partition; comparing the selected nibble against an entry in a predetermined table; modifying the nibble based on the comparison; applying a second nonlinear feedback shift register to the partition; applying a rotation matrix to at least one of the nibbles in the partition; and determining whether a predetermined number of twiddles has been applied to the partition (Leech Summary; Column 4 lines 14 – 57 and Column 6 lines 45 – 66 and Murphy Summary and Column 9 line 34 – Column 10 line 57).

16. Claims 8, 14, 22 and 28 are rejected applied as above in rejecting Claims 1, 9, 15 and 23. Furthermore, Leech in view of Murphy teaches determining a trajectory associated with each partition; and determining a ring associated with each trajectory (Leech Summary; Column 4 lines 14 – 57 and Column 6 lines 45 – 66 and Murphy Summary and Column 9 line 34 – Column 10 line 57).

17. Claims 10 and 24 are rejected applied as above in rejecting Claims 9 and 23. Furthermore, Leech in view of Murphy teaches determining a set of at least one possible trajectory; applying an S2 box each possible trajectory the set to generate an encrypted possible trajectory; comparing the encrypted possible trajectory the encrypted digital image; and determining at least one actual trajectory when the comparison finds a match (Leech Summary; Column 4 lines 14 – 57 and Column 6 lines 45 – 66 and Murphy Summary and Column 9 line 34 – Column 10 line 57).

18. Claims 4 and 18 are rejected applied as above in rejecting Claims 3 and 17. Furthermore, Leech in view of Murphy teaches wherein the minimum partition block size is less than a length of a cryptographic key and the maximum block size is less than the length of the cryptographic times the dimensionality of a product space associated with the second S box (Leech Summary; Column 4 lines 14 – 57 and Column 6 lines 45 – 66 and Murphy Summary and Column 9 line 34 – Column 10 line 57).

19. Claims 7, 12, 21 and 26 are rejected applied as above in rejecting Claims 6, 11, 20 and 25. Furthermore, Leech in view of Murphy teaches wherein the first non-linear feedback shift register comprises a non-linear feedback shift register number three and the second non-linear feedback shift register comprises a non-linear feedback shift register number four (Leech Summary; Column 4 lines 14 – 57 and Column 6 lines 45 – 66 and Murphy Summary and Column 9 line 34 – Column 10 line 57).

Conclusion

20. Examiner's Note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures

may apply as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

21. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892.

Applicant is urged to consider the references. However, the references should be evaluated by what they suggest to one versed in the art, rather than by their specific disclosure. If applicants are aware of any better prior art than those are cited, they are required to bring the prior art to the attention of the examiner.

22. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m.. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-232-3795. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy
September 07, 2005.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100